Distribution of integral points on varieties(Analytic Number Theory)

数理解析研究所講究録
886巻 1994年 39-47

Distribution of integral points on varieties

お茶の水女子大　藤原正彦
(Masahiko FUJIWARA)

次の合同式を考える。

$$G_i(X_1,\cdots,X_n)\equiv 0 \pmod p \qquad (i=1,\cdots,s)$$

ただし p は素数、G_i は整係数の form で次数 ≥ 2, $n\geq 4$

ここで我々が考察するのは、$\mathbb{R}^n$ に含まれる比較的に小さな箱 Q にある整数解の個数についてである。すなわち、

$$N=N(\underline{G},Q)=\#\{\underline{x}\in\mathbb{Z}^n\cap Q\,;\,\underline{G}(\underline{x})\equiv 0 \pmod p\}$$

$Q=[0,p)^n$ にとった時は、$\underline{G}\equiv 0 \pmod p$ の個数に他ならず、古典的な Lang-Weil (1964) の結果がある。

すなわち、

$G_1,\cdots,G_s$ が codim s の variety を定義している時は、

$$|N-p^{n-s}|<C\,p^{n-s-\frac{1}{2}}$$

ただし $C=C(n,s,d_1,\cdots,d_s)$ は p に無関係。

$\underline{G}$ がさらに non-singular mod p（すなわち、$\mathbb{Z}/(p)$ の代数的閉包の上で non-singular）ならば、

$$|N - p^{n-s}| < c\, p^{\frac{n-s+1}{2}}$$

というDeligne (1974) の結果がある。

Qが$[0, p)^n$より小さい時はどうであろうか。たとえば

① $G(\underline{x}) = x_1^d + \cdots + x_n^d$ (d even) の時、

$G(\underline{x}) \equiv 0 \pmod p$ $\underline{x} \neq 0 \Rightarrow |\underline{x}| \gg p^{\frac{1}{d}}$ だから、

Qを長さBの立方体とするとき $B \gg p^{\frac{1}{d}}$ となる。

② $G(\underline{x}) = (x_1^2 + \cdots + x_n^2)^{\frac{d}{2}}$ (d even) の時、

$G(\underline{x}) \equiv 0 \pmod p$ $x \neq 0 \Rightarrow |x| \gg p^{\frac{1}{2}}$ だから、

$B \gg p^{\frac{1}{2}}$ となる。

すなわち、Qを立方体とした時でさえ、$[0, p)^n$と比べて小さくし過ぎると、その中に$\underline{G} \equiv 0$の解が一つも入らなくなる可能性があるのである。

この論の中で、$\underline{G} = 0$は常にcodim sのvarietyを定義すると仮定する。また、いつも通り、$e_p(\alpha) = \exp\left(\frac{2\pi i \alpha}{p}\right)$とする。また、$Q = \{\underline{x} \in \mathbb{R}^n ; |x_i - a_i| < B_i\}$とする。ここで次の定義をする。

$\underline{G}$ が $P(p, k)$ を満たすとは、次が成立することとする。

$$^{\exists}c(\underline{G}) \quad {}^{\forall}\underline{u} \not\equiv 0 \pmod p$$

$$\sum_{\substack{\underline{y}=0 \\ p \mid \underline{G}(\underline{y})}}^{p-1} e_p(\underline{u}\cdot\underline{y}) < c(\underline{G})\, p^{n-k}$$

左辺の trivial estimate は $e_p(\ )=1$ とした時で、右辺は解の個数、すなわち $k=s$ となる。従って、$k \geq s$

(Th.) $\underline{G}$ が $P(p, k)$ を満たすとする。この時、

① $p \geq B_1, \cdots, B_n > {}^{\exists}c(n, \underline{d}, \varepsilon)$, $|Q| > {}^{\exists}c'(n, d, \varepsilon)\, p^{n+s-k}$
となるような箱 Q に対して、あるいは、

② 一辺が $B \geq p^{\frac{n+s-k}{n}}$ なる立方体 Q に対して、

$$N(\underline{G}, Q) \sim \frac{|Q|}{p^s}$$

が成立する。ただし $|Q|$ は Q の体積。

注 $\underline{G} \equiv 0 \pmod p$ の解の個数 $\sim p^{n-s}$ だから、もしこれらが一様に分布していると すると、Q 内に入る解の個数は $p^{n-s} \cdot \dfrac{|Q|}{p^n} = \dfrac{|Q|}{p^s}$ である。すなわち、上の定理は、$\underline{G} \equiv 0 \pmod p$ の解がかなり一様に分布し

ていることを意味している。証明は、FUJIWARA [4] と同様に進めればよい。

ここで問題となるのは、$P(p, \underline{G})$ の成立するような $\underline{G}$ の例である。

(例)① $\underline{G}$ を linearly non-singular mod p (すなわち、$\forall (a_1, \cdots, a_s) \not\equiv 0 \pmod p$, $a_1G_1 + \cdots + a_sG_s$ の最高次の part が non-singular mod p) とするとき、
$d_i \geq 2$ に対し、$P(p, \frac{n}{2})$ が成立する。
これは、Deligne (1973) による。

② $\underline{G}$ non-singular mod p, complete intersection, $d_i \geq 2$ とするとき、$P(p, \frac{n+s-1}{2})$ が成立する。
これは、Shparlinskii, Skorobogatov [9] による。

さて話を表題の integer solution に戻す。

$$N'(\underline{G}, B) = \{|\underline{x}| < B, \underline{G}(\underline{x}) = 0\}$$

とする。

$s = 1$ の時の trivial bound は B^{n-1} である。

$s=1$ の時には、他にも、 G absolutely irreducible の時、$N' < cB^{n-\frac{3}{2}}\log B$ (S. D. Cohen 1981), G が一次式を因子に持たない時、$N' < cB^{n-1-\frac{1}{n-1}}(\log B)^{2n}$ (Heath-Brown 1983), $G \neq (n-3)$ cylinder の時、$N' < cB^{n-1-\frac{5}{9}}$ (Schmidt 1986), G が non-singular の時、$N' < cB^{n-2+\frac{2}{n}}$ (FUJIWARA 1985), などの結果がある。 G がある条件を満たし、n が非常に大の時には、Hardy-Littlewood の方法が用いられ、$N' \sim B^{n-d}$ となる。

一般の G について、best bound はどの位だろうか。

$$G = X_1X_2^2 + X_3(X_4^2 + X_5^2 + \cdots + X_n^2)$$

とすると、$x_1 = x_3 = 0$, $x_2, x_4, \ldots, x_n$ 任意でよいから、$N' \geq B^{n-2}$。従って、$n-2$ より小さくなることはない。一方 $G = X_1X_2 - X_3X_4$ の解は $N' \sim B^2(\log B)^2$ であるから、best bound は、$B^{n-2}(\log B)^*$ ではないかと Serre は言っている。

(予想) codim s の variety を定義する $\underline{G}$ に対して、($d_i \geq 2$)

$$N' < B^{n-2s}(\log B)^*$$

は妥当かも知れない。

(Th.) $\underline{\underline{G}}$ — Ω が B の立方体。$\underline{\underline{G}}$ は密度 >0 の素数に対し $P(p, k)$ が成り立つとする。このとき、

$$N'(\underline{\underline{G}}, B) < c(n, \underline{\underline{d}}) B^{n-2s+\frac{ns+2s^2-2sk}{n+s-k}}$$

証明は、FUJIWARA [4] と同様に進めばよい。

(例) ① $\underline{\underline{G}}$ linearly nonsingular mod p for primes of positive density, $d_i \geq 2$

$$\Longrightarrow N'(\underline{\underline{G}}, B) < cB^{n-2s+\frac{4s^2}{n+2s}}$$

例えば、$d_i \geq 2$ で distinct, 各 G_i nonsingular なら linearly nonsingular for almost all p となるので、上の評価が成立する。

証明は、FUJIWARA [4]

② $\underline{\underline{G}}$ nonsingular, complete intersection, $d_i \geq 2$

$$\Longrightarrow N'(\underline{\underline{G}}, B) \leq cB^{n-2s+\frac{2s^2}{n+s-1}}$$

証明は Shparlinskii — Skorobogatov [9]. $s=1$ の時は $N' \leq cB^{n-2+\frac{2}{n}}$ となるが、この証明は、

FUJIWARA[ ] にある。

③ $\underline{G}$ に l 個の linear form が入っている時は、上の①，②は成立せず、次のように成る。

①で l コの linear form が入っている時、

$$N' \leq B^{n-2s+l+\frac{4(s-l)^2}{n+2s-3l}}$$

②で l コの linear form が入っている時、

$$N' \leq B^{n-2s+l+\frac{2(s-l)^2}{n+s-2l-1}}$$

㊟ ③で、$s=l$（すなわちすべて linear form）の時は、どちらも $N' \leq B^{n-l}$ となり、当然となる。　また $l=0$ の時は、①，②と同一になることから、当然の一般化と言えよう。

References

[1] S.D. Cohen. The distribution of Galois groups and Hilbert irreducibility theorem. Proc. London Math. Soc. (3), 43 (1981) 227–250

[2] P. Deligne. La conjecture de Weil I. Publ. Math. IHES., 43 (1974), 273–307

[3] M. FUJIWARA. Upper bounds for the number of lattice points on hypersurfaces. Number Theory and Combinatorics, edit. by Akiyama et al. (World Sci. Publ., Hong Kong, 1985), 89~96

[4] 〃 . Distribution of rational point on varieties over finite fields. Mathematika, Part 2 Vol 35 (1988), 155 — 171

[5] 〃 . Counting points in a small box on varieties, Proc. of the Japan Acad. Ser. A No. 8 Vol 64 (1988), 267–270

[6] D. R. Heath-Brown. Cubic forms in 10 variables. Proc. London Math. Soc. (3), 47 (1983), 225–257

[7] W. M. Schmidt. Small solutions of congruences. Diophantine Analysis, edit. by J.H. Loxton, A.J. Van der Poorten (Cambridge University Press, 1986).

[8] 〃 . Integer points on hypersurfaces. Mh. Math., 102 (1986), 27–58

[9] Shparlinskii, Skorobogatov, Exponential sums and rational points on complete intersections, Mathematika 37 (1990)